IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA,	)	
Plaintiff,	)	8:13CR106
	)	8:13CR107
	)	8:13CR108
	)	
vs.	)	
	)	
RUSSELL GLENN PIERCE, et. al.,	)	
JOHN DOE #1, et. al., and	)	
KIRK COTTOM, et. al.,	)	
Defendants.	)	
	)	

GOVERNMENT'S OMNIBUS POST-HEARING BRIEF IN OPPOSITION TO DEFENDANTS' MOTIONS TO SUPPRESS EVIDENCE

Prepared and Submitted by:

DEBORAH R. GILG
United States Attorney
for the District of Nebraska

MICHAEL P. NORRIS (#17765)
Assistant U.S. Attorney
1620 Dodge Street, Suite 1400
Omaha, Nebraska 68102-1506
Phone: (402) 661-3700

KEITH BECKER
DOJ Trial Attorney
1400 New York Ave NW 6th Floor
Washington, DC 20530
(202) 305-4104

SARAH CHANG
DOJ Trial Attorney
1400 New York Ave NW 6th Floor
Washington, DC 20530
(202) 353-4979

I. INTRODUCTION

Each defendant has moved to suppress evidence derived from the court-authorized deployment of a Network Investigative Technique ("NIT"), alleging that he was not timely notified of the warrant's execution pursuant to the requirements of Federal Rule of Criminal Procedure 41(f). There is no dispute that a copy of the warrant authorizing the NIT was provided to each defendant in this case. Suppression is inappropriate here because any alleged error in the timing of notice did not prejudice any defendant, involve any reckless disregard of proper procedures or otherwise raise any Constitutional issue. Accordingly, the defendants' motions should be denied.

II. FACTS

A. Search Warrants Authorizing the Network Investigative Technique

There are three search warrants pertinent to the pending motions, as noted on the chart below:

Case No.	Warrant No.	Authorized	Return filed	Hrg. Ex. #
13-CR-106	12-MJ-360	11/17/2012	11/20/2012	1
13-CR-107	12-MJ-356	11/15/2012	11/19/2012	2
13-CR-108	12-MJ-359	11/17/2012	11/20/2012	3

On each of those respective dates, the United States District Court for the District of Nebraska authorized a search warrant to allow law enforcement agents to deploy a NIT on one of three distinct child pornography websites in an attempt to identify the actual Internet Protocol ("IP") addresses and other identifying information of computers used to access the site. As

thoroughly described in the lengthy affidavits submitted in support of the warrants, the use of such a novel technique was necessitated by the defendants' use of websites that operated on the anonymous Tor network to exploit children while intending to avoid law enforcement detection. No defendant claims that there was a lack of probable cause to support the issuance of the warrants. The applications, affidavits, warrants and returns were admitted as hearing Exhibits 1-3.

Pursuant to the authorization for each warrant, each time a user of the site accessed any page in certain particularly described sections of the site, the NIT sent one or more communications to the user's computer, designed to cause the receiving computer to deliver to a computer known to or controlled by the government, data that would help identify the computer accessing the site, its location, its user, and other information about the computer. Ex. 1, Aff. ¶¶ 21-22.[1] That data included the computer's actual IP address and the date and time that the NIT determined what that IP address was, a unique session identifier to distinguish the data from that of other computers, and the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86). Id. at ¶ 22. The warrant affidavits articulated that the NIT did not deny the users access to any data or functionality of the computer. Id. at ¶ 21.

Each affidavit included a section titled, "REQUEST FOR DELAYED NOTICE," that cited and described the delayed notice provisions of Rule 41 and 18 U.S.C. § 3013a, articulated in detail why delayed notice was necessary, and requested authorization to delay notice to persons whose computers the NIT was used upon. Ex. 1, Aff. at ¶¶ 26-29. For instance, the

[1] While citations are to Exhibit 1, each of the warrants contained identical articulations regarding the operation of the

affidavits requested that the Court "authorize the proposed use of the NIT without the prior announcement of its use" because "[a]nnouncing the use of the NIT could cause the members of [the websites] to undertake other measures to conceal their identity, or abandon the use of [the websites] completely, thereby defeating the purpose of the search." Id. at ¶ 26. The affidavits articulated that notice of the use of the NIT "would risk destruction of, or tampering with, evidence, such as files stored on the computers of individuals accessing [the websites]" and therefore would "seriously jeopardize the success of the investigation into this conspiracy and impede efforts to learn the identity of the individuals that participate in this conspiracy, and collect evidence of, and property used in committing, the crimes (an adverse result under 18 U.S.C. §3103a(b)(l) and 18 U.S.C. § 2705)." Id. at ¶ 27. The affidavits further articulated that "the investigation has not yet identified an appropriate person to whom such notice can be given." Id. at ¶ 28. Accordingly, the affidavits requested "authorization, under 18 U.S.C. §3103a, to delay any notice otherwise required by Federal Rule of Criminal Procedure 41(f), until 30 days after any individual accessing [the website] has been identified to a sufficient degree as to provide notice, unless the Court finds good cause for further delayed disclosure." Id. at ¶ 29. (emphasis added). Further, in a section of the affidavit titled "SEARCH AUTHORIZATION REQUESTS," the affidavit reiterated its request that:

> pursuant to 18 U.S.C. § 3103a(b)(3), to satisfy the notification requirement of Rule 41(f)(3) of the Federal Rules of Criminal Procedure, the government may delay providing a copy of the search warrant and the receipt for any property taken for thirty (30) days after a user of an "activating" computer that accessed [the website] has been identified to a sufficient degree as to provide notice, unless notification is further delayed by court order.

NIT and the delayed notice requests.

Id. at ¶ 34 (emphasis added). The application for the search warrant also reiterated the request for delayed notice, which checked the appropriate box on the warrant application indicating that "[d]elayed notice of 30 days . . . is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet." Ex. 1, App. at p. 1. In each instance, the issuing magistrate judge granted that request, checking the box on the warrant itself to commemorate his finding that "immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial)," and authorizing "the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized for 30 days." Ex. 1, Warr. at p. 1 (emphasis added). The warrant did not authorize notice to any other person.

On November 19 and 20, 2012, each warrant was returned to the Court. Those warrant returns articulated that "[a] Network Investigative Technique (NIT), computer code, was installed on [the website] . . . ." Ex. 1, Warr. at p. 2.

B. Testimony of Special Agent Jeff Tarpinian

On April 17 and 18, 2014, this court heard testimony from Special Agent Jeff Tarpinian (SA Tarpinian) of the Federal Bureau of Investigation (FBI) regarding the three NIT search warrants, their execution, and delayed notifications given to named defendants in case numbers 13-CR-106, 13-CR-107, and 13-CR-108. SA Tarpinian testified that he has been a special agent with the FBI for approximately 26 years who, for the past five to six years, has been primarily assigned to investigate child exploitation matters. Hrg. Tr., Vol. 1, 34, 9-23. He summarized his training and experience investigating child exploitation matters, to include participation in nearly 100 investigations and the execution of nearly 100 search warrants. Id., 34, 20-23; 35, 1-18. SA Tarpinian was the lead investigator in the investigation of the child pornography websites

pertinent to the NIT warrants and described the background of the investigation for the Court. Id., 35-36. He was the affiant on each of the pertinent NIT warrants. See Ex. 1, 2 and 3.

For each warrant application, SA Tarpinian stated that he requested delayed notice regarding the execution of the warrant by checking the box marked "delayed notice of 30 days." See Hrg. Tr. Vol. 1, 40, 13-14 (regarding 12-MJ-360); id. at 45, 18-22 (regarding 12-MJ-356); id. at 48, 17-21 (regarding 12-MJ-359). SA Tarpinian also testified that to each warrant application was appended an affidavit in support of the search warrant and application, which included paragraphs titled "Request for Delayed Notice" and paragraphs titled "Search Authorization Requests" that sought and justified delayed notification under Rule 41 and 18 U.S.C. § 3103a. See Hrg. Tr. Vol. 1, 41-42 (regarding 12-MJ-360); id. at 46-47 (regarding 12-MJ-356); id. at 49-50 (regarding 12-MJ-359). In each affidavit, SA Tarpinian testified that he sought authorization to provide notice "30 days after any individual accessing [Website name] has been identified to a sufficient degree as to provide notice." See id. at 41, 16-18; 46, 15-17; 49, 21-23.

During his testimony, SA Tarpinian reviewed each warrant for the Court and pointed to each instance in which the authorizing court had granted the government's request for delayed notification without modification or limitation. See id. at 42, 15-25; 47, 5-14; 50, 12-19. See also Hrg. Exhibit 1, 1; Hrg. Exhibit 2, 43; Hrg. Exhibit 3, 2. SA Tarpinian also articulated his understanding of such authorizations, specifically as to when the delayed notice period was to begin. For example, regarding 12-MJ-360, SA Tarpinian testified that he understood that the "delayed notice period was to begin when the government identified the true name user of an individual that accessed one of these three websites." Hrg. Tr. Vol. 1, 43, 3-5.

SA Tarpinian explained through testimony how these identifications were made. The process involved a series of steps involving first, subpoenaing Internet Service Providers (ISPs) who owned the IP addresses returned by the Network Investigative Technique (NIT) for subscriber information. Hrg. Tr. Vol. 1, 55-56. Second, because the subscribers of the IP addresses may not be the actual users of the computers accessing the target websites, SA Tarpinian testified that: "Once we identify the residence where the subscriber's located, we will do what I say – sort of typical law enforcement background information." Hrg. Tr. Vol. 1, 56, 18-20. This consisted of determining who lives at or has access to the residence and applying for a search warrant of that residence. Id. at 56, 21-25. Through the execution of the warrant, SA Tarpinian stated that law enforcement sought to conduct an on-site preview of the digital media present in the home and interview all the occupants. Id. at 57, 3-15. These steps were taken to further aid law enforcement in identifying the individuals actually accessing the target websites.

SA Tarpinian testified that once sufficient identification was made through the above mentioned investigative steps, notice was provided to the named defendants through the discovery process. Hrg. Tr. Vol. 1, 59, 21-23. The form of the notice, as SA Tarpinian explained, was sometimes provided in the affidavits made in support of each residential search warrant, contained on the initial discovery disks prepared by SA Tarpinian sent to defense attorneys in each case. Hrg. Tr. Vol. 1, 68-71. In other instances, according to SA Tarpinian's testimony, notice was provided during identity or detention hearings held in the districts of arrest. Hrg. Tr. Vol. 1, 74-75; id. at 90-91. Additionally, some defendants received notice only after a full forensic examination was completed of their electronic media because the on-site previews and

interviews did not sufficiently identify anyone in the residence as the actual user of the target websites. Hrg. Tr. Vol. 1, 76-79; id. at 83-86; id. at 93-96.

III. **ARGUMENT**

The defendants contend that the government failed to comply with Rule 41 by not timely providing notice of the execution of the NIT warrant. The provision of notice of a search is at most a requirement of the criminal rules and not a requirement of the Fourth Amendment. See United States v. Simons, 206 F.3d 392, 403 (4th Cir. 2000) ("The Fourth Amendment does not mention notice, and the Supreme Court has stated that the Constitution does not categorically proscribe covert entries, which necessarily involve a delay in notice."); United States v. Pangburn, 983 F.2d 449, 455 (2d Cir. 1993) ("The Fourth Amendment does not deal with notice of any kind, but Rule 41 does."); United States v. Christopher, Crim. No. 2008-0023, 2009 WL 903764, at *7 (D.V.I. Mar. 31, 2009) ("The procedural requirements for giving notice after execution of a valid search warrant are ministerial tasks and a failure to comply therewith, without more, does not amount to deprivation of Fourth Amendment rights . . . .").

Because the exclusionary rule is a "blunt instrument," courts are "wary in extending [it] . . . to violations which are not of constitutional magnitude." United States v. Hornbeck, 118 F.3d 615, 618 (8th Cir. 1997) (quoting United States v. Burke, 517 F.2d 377, 386 (2d Cir. 1975)). Thus, noncompliance with Rule 41 "does not automatically require the exclusion of evidence in a federal prosecution." United States v. Spencer, 439 F.3d 905, 913 (8th Cir. 2006) (citing United States v. Schoenheit, 856 F.2d 74, 76 (8th Cir. 1988)). Rather, as the Eighth Circuit has recognized, when the government fails to comply with the requirements of Rule 41, exclusion is warranted only if: (1) the defendant can demonstrate that he was prejudiced by the

noncompliance, or (2) reckless disregard of proper procedures is evident. Spencer, 439 F.3d at 913; United States v. Nichols, 344 F.3d 793, 799 (8th Cir. 2003). Suppression is not the appropriate remedy here because none of the defendants can show prejudice or reckless disregard of proper procedures. Moreover, law enforcement agents acted in good faith in accordance with their articulated requests to the Court regarding when and to whom notice was to be given.

At the conclusion of the evidentiary hearing on the defendants' motions, the Court outlined a number of questions for the parties to address in post-hearing briefing. The government addresses those questions in turn.

A. Were any defendants entitled to notice of the execution of the NIT warrants?

The government concedes, consistent with the stipulation reached among those parties that signed it, that the Court may assume that the court/warrant authorizing deployment of the pertinent network investigative technique effected Fourth Amendment searches on activating computers, and that each defendant who has admitted via stipulation to being an owner of an activating computer which was located in his residence at the time the NIT effected a search was entitled to notice of the pertinent NIT warrant's execution.[2]

Defendant Tidwell has requested permission to "renounce" the stipulation he signed under penalty of perjury and argues that his computer was not the computer on which the NIT

[2] Those parties who have signed the stipulation have stipulated that:

> The court may assume that the court/warrant authorized deployment of the pertinent network investigative technique effected a Fourth Amendment search on an activating computer;
> At the time the NIT effected a search, each defendant owned an activating computer which was located in the Defendant's residence;
> The Government will not object to a defendant's claim of standing under the Fourth Amendment to challenge the execution of the pertinent NIT warrant; and
> Standing, as used in this stipulation, is understood and agreed to be a defendant's claim to a reasonable expectation of privacy in an area searched.

As the stipulation made clear, the parties do not stipulate and agree regarding the questions of whether any defendant has/had a reasonable expectation of privacy in the information collected pursuant to use of the NIT. The government

activated. 13-CR-106, Dkt. No. 173; Dkt. No. 191, pp. 1-2. "The Fourth Amendment protects the people against unreasonable searches of 'their' effects, and an accused in a criminal case may not assert the Fourth Amendment rights of a third party." United States v. Stringer, 739 F.3d 391, 396 (8th Cir. 2014) (citing Rawlings v. Kentucky, 448 U.S. 98, 104–06 (1980)); Rakas v. Illinois, 439 U.S. 128, 133–38 (1978). "To mount a successful motion to suppress, an accused must first establish that he personally has a legitimate expectation of privacy in the object that was searched." Stringer, 739 F.3d at 396.

Defendant Tidwell has no expectation of privacy in a computer that he claims he did not own or use. He presented no evidence at the April hearing to establish standing to challenge the execution of the NIT warrant. Accordingly, his argument means that he lacks standing to challenge the execution of the NIT warrant. See, e.g., Stringer, 739 F.3d at 396 (finding defendant lacked expectation of privacy in, and therefore standing to challenge evidence seized from, cell phone belonging to another defendant).

Defendant David Smith also claims that notice should have been provided to his father, James Smith, the Internet subscriber at his residence. 13-CR-108, Dkt. No. 144, pp. 8-9. David Smith may not assert the Fourth Amendment rights of another individual as a basis for establishing a violation of his rights. See United States v. Rodriguez-Arreola, 270 F.3d 611, 616 (8th Cir. 2001) (finding defendant "cannot use the violation of another individual's rights as the basis for his own Fourth Amendment challenge.") (citing United States v. Payner, 447 U.S. 727, 731 (1980)). Accordingly, his argument that notice should have been provided to James Smith is of no moment.

---

continues to contend that no defendant has any reasonable expectation of privacy in that data.

B. What is the notice the defendant was entitled to receive, and how was he entitled to receive it?

Pursuant to Rule 41, the defendants were entitled to receive a copy of the pertinent warrant authorizing the NIT deployment. Although the inventory forms were completed and provided to the Court and to each defendant in discovery, the defendants were not entitled to an inventory of items seized because no property was seized pursuant to the warrants. Each defendant was provided with that notice through the discovery process, when a copy of the pertinent NIT warrant, application and affidavit were provided to the defendants' attorneys.

Rule 41(f)(B), "Inventory," requires an officer to "prepare and verify an inventory of any property seized" pursuant to a search warrant. Rule 41(f)(C), "Receipt," requires an officer executing a warrant to "give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property." Rule 41 does not provide instructions regarding a receipt for property or inventory requirement where the search does not result in the seizure of property, nor does it require an inventory of property not seized pursuant to a warrant.

Because no seizure of any property took place pursuant to the NIT authorization, Rule 41 inventory requirements were not triggered. A seizure of property under the Fourth Amendment occurs when there is "some meaningful interference with an individual's possessory interests in that property." Dixon v. Lowery, 302 F.3d 857, 862 (8th Cir. 2002) (quotation marks and citations omitted). Not "every governmental interference with a person's property constitutes a seizure of that property under the Constitution." United States v. Va Lerie, 424 F.3d 694, 702 (8th Cir. 2005) (en banc). The Fourth Amendment only prohibits the government's "conversion

of an individual's private property" rather than "mere technical trespass to an individual's private property" or "inconsequential interference with an individual's possessory interests." Id.

The NITs did not meaningfully interfere with any defendant's possessory interests. The NITs merely collected information – the computer's actual IP address and the type of operating system running on the computer – in which the defendants had no reasonable expectation of privacy. See United States v. Suing, 712 F.3d 1209, 1213 (8th Cir. 2013) (defendant "had no expectation of privacy in [the] government's acquisition of his subscriber information, including his IP address and name from third-party service providers.") (citing United States v. Stults, 575 F.3d 834, 842 (8th Cir. 2009) and United States v. Perrine, 518 F.3d 1196, 1205 (10th Cir. 2008)).

"IP addresses are numbers that are automatically assigned when a person[] signs onto the internet via an 'ISP' (Internet Service Provider). Thus when a person uses an internet service provider to access the internet, that person is assigned an IP address unique to the 'session' in which he is signed on to the internet." United States v. Hair, 178 Fed.Appx. 879, 883, 2006 WL 1073056 at *2, n. 4 (11th Cir. 2006). IP addresses may be "static," in that they remain constant, or "dynamic," in that they change periodically. See Kilman v. Comcast Cable Comm., Inc., 465 F.3d 271, 273 (6th Cir. 2006). The IP address provides basic routing information a user needs to contact and access a particular computer on the Internet, to include a website or information stored thereon. Peterson v. Nat. Tel. and Inf. Admin., 478 F.3d 626, 629 (4th Cir. 2007). IP addresses belong to Internet Service Providers, not to any of the defendants, and are assigned to an Internet subscriber to allow that subscriber to access the Internet. Hrg. Tr. Vol. 1, 55-56.

By its nature, an IP address is accordingly not something that can be seized from a defendant's computer or home. The NIT merely recorded a user's IP address and operating system type and did not deny any defendant access to or functionality of his computer. Such a recording of information does not constitute a seizure. See Arizona v. Hicks, 480 U.S. 321, 324 (1987) (recording of stereo equipment serial number while present in home is not a "seizure" because it did not meaningfully interfere with defendant's possessory interest in the serial number or equipment).

Accordingly, without respect to the timing issues discussed herein, providing each defendant with a copy of the pertinent NIT warrant was sufficient to comply with Rule 41 obligations and no inventory was required. Yet, even assuming that the government improperly filled out the inventory sheet, or failed to provide a proper inventory, such a ministerial violation does not warrant suppression absent a showing of prejudice or reckless disregard of proper procedures. See Nichols, 344 F.3d at 799 (affirming denial of suppression motion where defendant failed to establish prejudice from claimed inadequacies in search warrant inventory list). In Nichols, the defendant made the same argument that defendants present here: that exclusion is the proper remedy when officers fail to provide a comprehensive inventory of items seized as required under Rule 41. See Nichols, 344 F.3d at 799. Without a showing of prejudice, the Eighth Circuit in Nichols concluded that the defendant could not prevail. Id.

Some defendants claim, absent any supporting authority, that providing a copy of the NIT search warrant, application and affidavit to their attorneys as opposed to the defendants themselves was somehow insufficient notice. A criminal attorney is an agent of the defendant whose acts may bind the defendant. See United State v. Suarez, -- Fed. Appx. --, 2014 WL

1716719 at * 2 (8th Cir. May 2, 2014) ("For certain rights, 'waiver may be effected by action of counsel,' in which case 'the defendant is deemed bound by the acts of his lawyer-agent and is considered to have notice of all facts, notice of which can be charged upon the attorney.'"). Moreover, directly providing such notice to a represented party, rather than the party's representative, could implicate Fifth or Sixth Amendment concerns as well as ethical issues regarding contact with represented persons. Any asserted delay caused by that attorney failing to promptly provide a copy of discovery materials to his client cannot be attributed to the government.

C. When was each defendant required to receive such a notice?

A defendant was entitled to receive notice no sooner than 30 days from when a user of an activating computer was identified to a sufficient degree to provide notice, as articulated in the affidavits made in support of the warrants. In the event that such an understanding on behalf of law enforcement was incorrect, the clear, specific articulation of that understanding in the affidavits demonstrates good faith on behalf of the executing agents and a lack of any reckless or intentional disregard of proper procedures.

Rule 41(f)(3) allows for the delay of any notice required by Rule 41 "if the delay is authorized by statute." 18 U.S.C. § 3103a(b) allows for any such notice to be delayed if:

> (1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705, except if the adverse results consist only of unduly delaying a trial);
> (2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and

> (3) the warrant provides for the giving of such notice within a reasonable period not to exceed 30 days after the date of its execution, or on a later date certain if the facts of the case justify a longer period of delay."[3]

Here, the issuing magistrate granted the government's request that notice of the NIT warrant be delayed for 30 days "after a user of an 'activating' computer that accessed [the website] [had] been identified to a sufficient degree as to provide notice." Ex. 1, ¶ 29. A copy of the NIT warrant was then provided to all defendants through discovery.

Defendants have argued that the notice clock began to run at various points, to include 30 days from: the warrant's return (on November 19 or 20, 2012); the identification of IP addresses by the NITs; or the receipts of a subpoena return identifying a name and address of the subscriber to an Internet service account associated with such an IP address. To give proper notice at any of those points was not possible, however, because law enforcement did not yet have the information required to provide notice to the proper persons.

The NIT merely identified IP addresses of computers that accessed the websites on the respective dates charged. An IP address is not a person to whom notice can be given. In fact, the NIT did not identify any person, the user of an activating computer or the computer itself – it only identified an IP address and operating system type of a computer used to access the website. That information is helpful, but not nearly sufficient, to identify the actual user of the computer or the computer that activated the NIT.

---

[3] Under 18 U.S.C. 2705(2), any of the following constitute an adverse result:
(A) endangering the life or physical safety of an individual;
(B) flight from prosecution;
(C) destruction of or tampering with evidence;
(D) intimidation of potential witnesses; or
(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

Subscriber information contained in the respective subpoena returns from Internet Service Providers (ISPs) is also helpful, but not sufficient, to identify the actual user of the computer or the searched computer. As SA Tarpinian testified, subpoena returns from ISPs provided "the subscriber to that IP address and . . . frequently the subscriber is not the user of the computer that is involved in the investigation . . . . There isn't necessarily a direct connection, if you will, between the subscriber and who law enforcement ultimately determines is behind the keyboard." Hrg. Tr. Vol. 1, 56, 4-13. Further investigation, to include a search of the defendants' residences, interviews of suspects, and either preliminary or full computer forensic examinations of suspect computers was necessary before a determination could be made as to the actual identity of the users behind the computers that accessed the websites on the pertinent date or dates charged in the Indictments. See Hrg. Tr. Vol 1, 56-57. Moreover, providing notice to the subscriber of an internet service account -- who may or may not be the actual user of the computer that activated the NIT – would have been inconsistent with the requirement to provide notice "to the person who, or whose property, will be searched" as reflected on the warrant. And in many cases – including those of defendants Pierce, Peer, Laurita, Moore, and Smith – would have resulted in notice being provided to the wrong person. Only after interviewing defendants, preliminarily searching their residences and computers – and, in some cases, conducting a full computer forensic examination – did law enforcement agents sufficiently identify them as the individuals who actually accessed the websites. Accordingly, at the earliest, notice could be given at the date of the respective residential searches and arrests, or after a full forensic examination tied a person to activity on the pertinent website.

D. When did each defendant actually receive notice, and what was the notice?

The following chart illustrates the dates on which each defendant had his residence searched, was arrested, was provided notice of the NIT warrant, and the form of notice received by each defendant. See. Ex. 50.

Defendant	**Resid. SW**	**Arrest**	**Notice Date**	**Form of Notice**
Russell Pierce	4/8/13	4/8/13	5/16/13	Discovery materials
David Peer	4/9/13	4/9/13	6/3/13[4]	Discovery materials
Warren Tidwell	4/9/13	8/22/13	9/10/13	Discovery materials
Joshua Welch	4/9/13	4/9/13	4/11/13 5/28/13	Detention hearing testimony Discovery materials
Thomas Spencer	4/11/13	4/11/13	5/9/13	Discovery materials
Vincent Diberardino	4/9/13	4/9/13	5/16/13	Discovery materials
Mike Huyck	4/9/13	4/9/13	4/26/13	Discovery materials
Anthony Laurita	4/9/13	11/18/13	11/25/13	Discovery materials
Brandon Moore	4/9/13	4/9/13	5/13/13	Discovery materials
John Sebes	4/10/13	4/10/13	5/16/13	Discovery materials
Gary Reibert	4/8/13	4/8/13	5/16/13	Discovery materials
Kirk Cottom	4/9/13	4/9/13	4/11/13 5/17/13	Identity and detention hearing testimony Discovery materials
David Smith	4/11/13	11/15/13	12/17/13	Discovery materials
Kevin Pitman	4/9/13	4/9/13	4/9/13 5/29/13	Initial appearance filings Discovery materials

Discovery materials provided to all defendants included a copy of the pertinent NIT warrant, application, affidavit and return, in addition to further materials describing the particular information collected regarding each defendant's computer. In most cases, defendants were provided with NIT notice through discovery within or nearly 30 days after a residential search and related investigation, to include subject and witness interviews and preliminary computer forensic examinations that disclosed sufficient information to identify the defendant as the user who accessed the pertinent website, in which event the defendant was arrested.

Defendants Tidwell, Laurita and Smith were not arrested on the date of the search of their respective residences. On the date Defendant Tidwell's residence was searched, he was interviewed by law enforcement and denied knowledge of the network on which the pertinent website operated and denied viewing child pornography during his interview. Hrg. Tr. Vol. 1, 76. Defendant Tidwell also suggested that another person had had access to his computer and later named that person to law enforcement. Id. As SA Tarpinian testified, a preliminary examination of Defendant Tidwell's digital media did not reveal any conclusive evidence tying Defendant Tidwell to the use of "Website A." Id. Only after a full forensic examination of seized digital media was law enforcement able to confirm that Defendant Tidwell was the user of the pertinent website. Hrg. Tr. Vol. 1, 76-79. As SA Tarpinian explained, a full forensic analysis of Defendant Tidwell's Kindle tablet revealed internet history files that showed network activity, including activity on the website in question, indicating that the user of the Kindle had accessed that website. Id. at 78-79; see Ex. 13. That additional information provided a basis to believe that Defendant Tidwell was, in fact, the user who accessed the pertinent website on the date in question and, accordingly, the proper person to whom notice was due. Defendant Tidwell was subsequently indicted and notice was provided to his attorney through discovery.

With respect to Defendant Laurita, SA Tarpinian explained that agents were unable to confirm that he was the user of the pertinent website at the time of the search of his residence. Hrg. Tr. Vol. 1, 83. Defendant Laurita's interview did not disclose definitive information tying him to the website and, more importantly, a forensic examination was not conducted at the residence. Id. After a full forensic examination of digital media seized from the residence, law

[4] As reflected in his docket, Defendant Peer was in transit from the State of Utah to Nebraska for some time, and

enforcement was able to confirm that Defendant Laurita was the user who had accessed the website. SA Tarpinian testified that the completed forensic report of Defendant Laurita's electronic devices showed evidence of child pornography activity as well as network activity on which the website in question operated. Hrg. Tr. Vol. 1, 84-85; Ex. 29. Laurita was subsequently indicted and arrested, and notice was provided to him through the discovery process given to counsel.

Defendant Smith also received notification of the NIT warrant upon his later indictment and arrest, which occurred after a full forensic examination was completed on digital media seized from his residence. As SA Tarpinian explained, not all occupants of the home could be interviewed at the time of the search and the home contained at least thirty-eight electronic devices, including three computers that each contained multiple hard drives. Hrg. Tr. Vol. 1, 94-95. No preliminary forensic examination was done at the time of the search. While defendant Smith made some relevant admissions, his interview did not conclusively show him to be the user who accessed the website in question. In addition, as SA Tarpinian testified, because Defendant Smith's mother was running a day care at the residence, law enforcement's first priority was to address whether or not any of those children were being victimized. Hrg. Tr. Vol. 1, 93. Thus, "a determination was made to . . . seize the digital media there, wait for a comprehensive forensic examination and then go forward after results were received." Id. at 94, 1-3. Full forensic examination ultimately tied child pornography evidence to Defendant Smith's devices as well as found network activity on which the website in question operated. Id. at 95.

---

notice was provided shortly after he was assigned counsel upon arriving in Nebraska.

The NIT's authorization and use, as well as the information collected pursuant to it, was disclosed to Defendants Welch, Cottom and Pitman shortly after their respective arrests. For example, Defendant Welch received notification about the NIT warrant during his detention hearing held on April 11, 2013 when the case agent provided testimony describing the use of the NIT to derive Defendant Welch's IP address. See Ex. 17. Both Defendants Cottom and Pitman were arrested on the day residential searches were conducted at their homes. Defendant Cottom received notice of the NIT warrant shortly thereafter during his identity and detention hearing in the Western District of New York through agent testimony adduced at the hearing. See Ex. 39. Defendant Pitman also received notice of the NIT warrant shortly after his arrest, following the filing of a criminal complaint on April 9, 2013 charging him with child pornography offenses. He had his initial appearance in the Western District of Texas where a copy of his arrest warrant, criminal complaint and the affidavit in support of that complaint were filed on the public docket. Within the affidavit in support of that complaint is a detailed account of the use of the NIT to identify Defendant Pitman's IP address. See Ex. 43.

E. If the defendant did not receive timely notice, what specific prejudice did that defendant suffer?

Prejudice, for the purposes of this inquiry, means "that the search might not have occurred or would not have been so abrasive if the Rule had been followed." United States v. Burgard, 551 F.2d 190, 193 (8th Cir. 1977) (quoting Burke, 517 F.2d at 386-87); see also, Schoenheit, 856 F.2d at 77; United States v. Brown, 584 F.2d 252, 258 (8th Cir. 1978). The defendants do not, and cannot, make such a showing. The warrant on its face authorized a delay in notice until after the search took place. Accordingly, the search would have occurred regardless of any delay in providing notice. Moreover, the search would have resulted in the

collection of the exact same data – i.e., been just as "abrasive" – even if notice had been provided within 30 days from any of the dates when the defendants claim notice should have been given. Further, each defendant received notice of the NIT warrant in sufficient time to have a full opportunity to challenge the issuance and execution of the warrant before this Court. Thus, the defendants did not suffer any actual prejudice from any delayed notice.

The denial of motions to suppress has routinely been upheld where a defendant fails, as here, to establish prejudice from a failure in the execution of a search warrant. See Nichols, 344 F.3d at 799 (affirming denial of suppression motion where defendant failed to establish prejudice from claimed inadequacies in search warrant inventory list); United States v. Reisselman, 646 F.3d 1072, 1078 (8th Cir. 2011) (affirming denial of suppression motion where defendant failed to establish prejudice from officer's failure to provide warrant attachment to defendant at time of search).

Defendant Tidwell claims he was prejudiced because earlier notice could have allowed him to identify sooner the person whose computer he claims actually activated the NIT. As noted earlier, the import of Defendant Tidwell's argument is that he lacks standing to challenge the execution of the NIT warrant. See, e.g., Stringer, 739 F.3d at 396 (finding defendant lacked expectation of privacy in, and therefore standing to challenge evidence seized from, cell phone belonging to another defendant). In any event, it is the defendant's burden to establish prejudice. Spencer, 439 F.3d at 913. Defendant Tidwell offered no evidence to support the core of his asserted factual conclusion – which appears to be that it was, in fact, a Macintosh computer

which he claims not to own, that activated the NIT.[5] Accordingly, his prejudice argument is either moot or factually unsupported.

Defendant Reibert contends that he was prejudiced because "several computers and devices likely accessed his internet service," "Internet routers are designed to allow multiple users within a network range to access the same internet service, and are frequently 'hacked' by unauthorized users" and therefore "he is unable to fully defend against the allegations, including presenting evidence of unauthorized use of his network access." 13-CR-107, Dkt. No. 234, p. 4. It is the defendant's burden to establish prejudice. Spencer, 439 F.3d at 913. Defendant Reibert presented no evidence whatsoever during the April hearing to support any of those asserted facts and hypothetical conclusions. Nor does Defendant Reibert offer any explanation as to why all of those facts and conclusions cannot be presented at trial, through fact and expert testimony, in support of such an asserted defense. Accordingly, his prejudice argument is unavailing.

F. If there was a failure to provide timely notify, did such a failure constitute a reckless disregard of proper procedures requiring the suppression of evidence?

Whether agents acted in reckless disregard of proper procedures is essentially a bad faith inquiry. See United States v. Bieri, 21 F.3d 811, 816 (8th Cir. 1994) ("[B]ecause no evidence exists that the officers acted in bad faith, it follows that there was no reckless disregard of proper procedure by the state officers."); United States v. Hyten, 5 F.3d 1154, 1157 (8th Cir. 1993) ("our prior determination that [agents] acted in good faith precludes any finding of reckless disregard of proper procedure on their part."); United States v. Berry, 113 F.3d 121, 123 (8th Cir. 1997)

[5] That conclusion itself appears to be based upon a misreading of information provided in discovery; in any event, it is the defendant's burden to establish facts to support his prejudice argument.

(holding officers lack of bad faith in executing warrant at night without proper provision in warrant meant officers did not act in reckless disregard of proper procedure).

The fact that law enforcement acted consistent with its articulated requests to the issuing magistrate demonstrates its good faith in how and when notice was provided. There is no indication of any bad faith on behalf of the agents here. To the contrary, the search warrant affidavits specifically and explicitly articulated that "the investigation has not yet identified an appropriate person to whom such notice can be given" as well as the need for and request to delay notice "for thirty (30) days after a user of an 'activating' computer that accessed [the website] has been identified to a sufficient degree as to provide notice." Nothing was hidden from the magistrate – to the contrary, the government specifically articulated its understanding that the thirty days would begin once a user was sufficiently identified. That explicit, articulated request demonstrates good faith on behalf of the agents. See United States. v. Mutschelkunaus, 592 F.3d 826, 830 (8th Cir. 2010) ("the officers' explicit request for an extension [of time to examine a computer pursuant to search warrant] shows a manifest *regard* for the issuing judge's role in authorizing searches, rather than a bad faith [attempt] to circumvent federal requirements." (emphasis in original) (internal citations omitted)). Moreover, notice was in fact provided to the defendants upon their identification as the proper person to whom notice was to be given.

The defendants have contended that the articulation in the affidavits regarding when the delay in notice would begin could not modify the warrants themselves. Yet, that argument misses the point. Even if law enforcement was mistaken in its understanding that the delayed notice timeline began when the correct person to whom notice could be given was identified, the

articulation of that understanding in the warrant documents demonstrates law enforcement's good faith in the execution of the warrants.

Numerous defendants contend that the government's reckless disregard of proper procedures is evident from a pattern by which notice was delayed. In the first instance, to establish bad faith, it is the defendant's burden to show that law enforcement did something beyond mere negligence in order to prejudice the defendant's defense or to otherwise put the defendant at a disadvantage. See United States v. Webster, 497 F.Supp.2d 966, 972 (S.D. Iowa 2007) (citing California v. Trombetta, 476 U.S. 479, 488 (1986)); see also id., at 973, n.15 (listing cases in the context of evidence destruction stating that the majority of courts have found that bad faith requires more than gross negligence or reckless behavior); Boykin v. Leapley, 28 F.3d 788, 793 (8th Cir. 1994) (finding no bad faith existed even though police acted negligently in their storage of a blood sample because defendant could not show any prejudicial effect from the state's failure to preserve evidence.); United States v. Scoggins, 992 F.2d 164, 167 (8th Cir. 1993) (finding no due process violation where law enforcement destroyed evidence pursuant to department policy and after obtaining a court order.). The Eighth Circuit has never held that a pattern of negligent conduct infers the presence of bad faith. See, e.g., United States v. McKinney, 395 F.3d 837, 841-42 (8th Cir. 2005) (holding that a clerical filing error did not establish bad faith or a pattern of negligence without expanding upon what constitutes a "pattern of negligence."). In any event, no defendant points to any advantage or gain to law enforcement from providing notice subsequent to identifying the person to whom notice should have been directed. In fact, the articulated reasons supporting the request for delayed notice – that "[a]nnouncing the use of the NIT could cause the members of [the websites] to undertake other

measures to conceal their identity, or abandon the use of [the websites] completely, thereby defeating the purpose of the search" and that notice of the use of the NIT "would risk destruction of, or tampering with, evidence, such as files stored on the computers of individuals accessing [the websites]" and therefore would "seriously jeopardize the success of the investigation into this conspiracy and impede efforts to learn the identity of the individuals that participate in this conspiracy, and collect evidence of, and property used in committing, the crimes (an adverse result under 18 U.S.C. §3103a(b)(l) and 18 U.S.C. § 2705)" are the exact reasons why notice was, in fact, given subsequent to the identification of the person to whom notice was given. Those very same reasons supported the coordination of residential searches, as articulated by Special Agent Tarpinian at the hearing. See Hrg. Tr. Vol. 1, 59, 10-15.

The analysis of the court in United States v. Christopher, 2009 WL 903764 (D. V.I., 2009), is instructive here. In Christopher, the government sought and was subsequently granted a 30-day delayed-notice search warrant authorizing an actual entry into a shack on a defendant's property. See Christopher, 2009 WL 903764 at *1. The government ultimately provided notice of the warrant at the defendant's arraignment, more than 60 days after the authorization of the warrant. Id. at * 6. The defendant moved to suppress based in part upon the failure to comply with the delayed-notice provision. In determining that suppression was inappropriate, that court found it "difficult to accept the proposition that a search may be deemed reasonable, and therefore constitutional, during the various stages of application for authorization, execution, and termination, only to be invalidated because of the operation of some condition subsequent, to-wit, a failure to provide notice" Id. at *7 (citing United States v. Cafero, 473 F.2d 489, 499 (3d Cir. 1973) ("We find it difficult to accept the proposition that a search may be deemed

reasonable, and therefore constitutional during the various stages of application for authorization, execution, supervision of the interception, and termination, only to be invalidated *ab initio* because of the operation of some condition subsequent, to-wit, a failure to give notice of the items seized"). Further, although the government did not apply for an extension of the delayed-notice provision, the court found "there was an implied extension of the delayed notice search warrant" when the court granted a subsequent order authorizing video surveillance of that defendant, in consideration of the "ongoing nature of the investigation" and the "need for further investigation to determine (1) the scope of the illegal activity and (2) the identify and roles of the participants." Id. at *7. That court further found that notice provided to the defendant "on the day of his arraignment was reasonable under the circumstances" of the case. Id.

Here, there is no question that the NIT warrant was issued upon an unchallenged finding of probable cause and that the Court approved the well-supported request for delayed notice. As in Christopher, notice was provided to each defendant through the criminal discovery process once a prosecution was initiated. This Court should find, as did the court in Christopher, that the notice provided here was reasonable under the circumstances.

Some defendants have suggested an inappropriate motive on behalf of the government on account of the fact that notice, with respect to each defendant, occurred subsequent to an arrest on probable cause. To the extent that is correct, such a pattern displays both consistency and judicial involvement in the notice decision. Each arrest of each defendant was followed by an identity hearing and judicial finding probable cause to support the arrest, or was preceded by a Grand Jury finding of probable cause, after which finding notice was provided. Rather than the sort of untrammeled discretion that the defendants contend law enforcement exercised, notice

therefore followed identifications sufficient to support independent findings of probable cause by the judiciary that the defendant was in fact the person who had accessed the pertinent website – and, accordingly, was the correct person to whom notice was to be provided.

Defendants have also asserted that the delay from the time a subpoena return was received identifying a residential Internet account subscriber and when a search of that residence was conducted suggests bad faith on behalf of law enforcement. As SA Tarpinian explained, at Hrg. Tr. Vol. 1, 59, such a delay was necessary in part because searches of subject addresses were coordinated throughout the country, in an effort to avoid the possibility of suspects gaining notice of law enforcement's infiltration into the subject websites and potentially advising others, which could lead to flight from prosecution and destruction of evidence. Those reasons are the same reasons articulated to, and approved by, the issuing magistrate to support the delay in notice to defendants in the first instance. Rather than evidencing any bad faith on behalf of law enforcement, accordingly, such reasons indicate that law enforcement again acted within the ambit of its articulated reasons for delaying notice.

G. **Any Delay in the Notice of a Warrant is not a Constitutional Violation**

In an effort to re-frame the issue of notice under Rule 41 as a substantive Fourth Amendment issue, various defendants claim via a multitude of theories that the alleged delay in providing notice of the NIT warrant rises to a constitutional violation. All of those arguments are unpersuasive.

Notice requirements are ministerial not Constitutional. See Simons, 206 F.3d at 403 ("The Fourth Amendment does not mention notice, and the Supreme Court has stated that the Constitution does not categorically proscribe covert entries, which necessarily involve a delay in

notice."); Pangburn, 983 F.2d at 455 ("The Fourth Amendment does not deal with notice of any kind, but Rule 41 does."); Christopher, 2009 WL 903764, at *7 (D.V.I. Mar. 31, 2009) ("The procedural requirements for giving notice after execution of a valid search warrant are ministerial tasks and a failure to comply therewith, without more, does not amount to deprivation of Fourth Amendment rights . . . .").

Some defendants claim that notice of a search warrant is a constitutional requirement, by means of an analogy to the Supreme Court's decision in Wilson v. Arkansas, 514 U.S. 927, 930 (1995). Wilson, which involves the common-law 'knock-and-announce' rule that the Supreme Court found to be properly part of a Fourth Amendment reasonableness inquiry, is inapposite here. In Wilson, the Supreme Court addressed only the knock-and-announce rule, finding that "the reasonableness of a search of a dwelling may depend in part on whether law enforcement officers announced their presence and authority prior to entering." Id. at 931(emphasis added).[6] Wilson did not involve Rule 41 notice or delayed notice requirements nor did it address searches in an online context. In fact, the Supreme Court's discussion of the common-law history of the knock-and-announce rule makes it clear that the rule is directed only at the physical entrance to a dwelling, where the Fourth Amendment protections are at their highest. See id. at 931-36. By contrast, neither the Fourth Amendment nor Rule 41 requires an officer executing a search warrant to present the property owner with a copy of the warrant before conducting his search. See United States v. Grubbs, 547 U.S. 90, 98-99 (2006). No law enforcement officer entered any defendant's dwelling pursuant to the NIT warrant.

[6] Even in Wilson, the Supreme Court recognized that "[t]he Fourth Amendment's flexible requirement of reasonableness should not be read to mandate a rigid rule of announcement that ignores countervailing law enforcement interests." 514 U.S. at 934.

Courts have, in fact, recognized for decades before the enactment of the delayed-notice provisions of Rule 41 and 18 U.S.C. § 3103a that surreptitious, delayed-notice searches were constitutional. See Dalia v. United States, 441 U.S. 238 (1979) (rejecting the argument that covert entry of a premises pursuant to a judicial warrant is unconstitutional as "frivolous"); Freitas, 800 F.2d at 1456-57; United States v. Villegas, 899 F.2d 1324, 1334-37 (2d Cir. 1990) (holding that "the tolerable limit was not exceeded," explaining that for "good cause, the issuing court may thereafter extend the period of delay."); United States v. Simons, 206 F.3d 392, 402-03 (4th Cir. 2000) (making clear that failure to provide notice of a search does "not render the search unreasonable under the Fourth Amendment."). It was clear long before the enactment of the USA PATRIOT ACT that judges have the authority to authorize delay in giving the notice of a search warrant's execution required by Rule 41.

Some defendants argue that the alleged delay in notice represents a "fundamental" violation of Rule 41 which is therefore of constitutional import, citing United States v. Freeman, 897 F.2d 346, 350 (8th Cir. 1990) (upholding denial of motion to suppress evidence obtained from a search warrant applied for and executed by affiant who was not authorized to apply for a search warrant, refusing to apply the exclusionary rule to "procedural violations which do not implicate the constitutional values of probable cause or description with particularity of the place to be searched and items to be seized."). In Freeman, the Eighth Circuit recognized that courts in multiple federal circuits had generally refused "to apply the exclusionary rule to violations of Rule 41 provisions, absent a constitutional infirmity or showing or prejudice or reckless disregard." Id. at 349 (citing cases). Rather, only a "fundamental" violation of Rule 41 would require automatic suppression, which the court defined as only one which "in effect, renders the

search unconstitutional under traditional fourth amendment standards." Id. at 350. In determining that no such fundamental violation occurred even in a "close case" where an unauthorized person had applied for and executed a warrant, the court found that the search was carried out in good faith, and "the affidavit supporting the search warrant provided probable cause to search and the search warrant described with particularity the place to be searched and the items to be seized." Id. The court also noted that the defendant suffered no prejudice in the sense that the search would not have occurred or have been so abrasive had proper procedural requirements been followed. Id.

Nothing about Freeman supports any argument that a fundamental Rule 41 violation occurred in this case. As in that case, here, the affidavit supporting the search warrant provided probable cause to search and the search warrant described with particularity the place to be searched and the information to be collected. Those core Fourth Amendment values were accordingly protected. Moreover, as argued herein, law enforcement acted in good faith in applying for and executing the warrant authorizing the NIT.

The nature of the search and the information collected is also pertinent to the Court's analysis of any Fourth Amendment interests at stake pursuant to the NIT warrant. All of the cases the defendants point to in support of their arguments about the fundamental Fourth Amendment character of the notice requirement involve actual entries into a person's home. No law enforcement officer entered any defendant's home pursuant to the NIT. Nor did the NIT even search any defendant's computer in a conventional sense – it did not provide access to computer files, folders, file structure, or information on the computer itself. The NIT merely

delivered IP and operating system information – information over which the defendants do not have a reasonable expectation of privacy – to a government computer. See supra Section IIIB.

The distinction drawn between levels of intrusion is one that Courts have recognized in terms of analyzing Fourth Amendment interests. For instance, the Second Circuit in Villegas described a covert entry into one's home as:

> less intrusive than a conventional search with physical seizure because the latter deprives the owner not only of privacy but also of the use of his property. It is less intrusive than a wiretap or video camera surveillance because the physical search is of relatively short duration, focuses the search specifically on the items listed in the warrant, and produces information as of a given moment, whereas the electronic surveillance is ongoing and indiscriminate, gathering in any activities within its mechanical focus.

899 F.2d at 1337. The NIT deployment, considering its short duration, the extremely limited set of information it collected, and that it produced only information as of the given moment it activated, is far less intrusive even than the already limited physical entry into a home described in Villegas.

IV. **CONCLUSION**

Each defendant was provided notice of the execution of the NIT warrant and, even if that notice was not timely, no defendant can establish any prejudice or reckless disregard of the notice procedures of Rule 41 and 18 U.S.C. § 3103a or that the delay in notice implicated any Constitutional interest. Accordingly, the Court should deny Defendants' motions to suppress.

WHEREFORE, the United States respectfully prays this Honorable Court to deny the Defendants' motions to suppress in this case.

Respectfully submitted,

__/s_____
MICHAEL P. NORRIS
ASSISTANT U.S. ATTORNEY

__/s_____
SARAH CHANG
TRIAL ATTORNEY

__/s_____
KEITH BECKER
TRIAL ATTORNEY

CERTIFICATE OF SERVICE

I hereby certify that I have caused a copy of this motion to be sent to counsel of record for all defendants in cases 13-CR-106, 107 and 108 via the Court's ECF system on June 6, 2014.

____/s_____
SARAH CHANG
TRIAL ATTORNEY